

DEVELOPMENT OF A SOFTWARE SAFETY PROCESS AND A CASE STUDY OF ITS USE

**Annual Progress Report
Grant No. NAG-1-1123**

August 1, 1995 - July 31, 1996

Submitted to:

**National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-0001**

Attention: Dr. Dave E. Eckhardt, MS 478

Submitted by:

**J. C. Knight
Professor**

**SEAS Report No. UVA/528344/CS97/106
November 1996**

DEPARTMENT OF COMPUTER SCIENCE

**SCHOOL OF
ENGINEERING 
& APPLIED SCIENCE**

**University of Virginia
Thornton Hall
Charlottesville, VA 22903**

INTRODUCTION

This is the annual report for the period August 1, 1995 to July 31, 1996 for NAG-1-1123. The principal investigator on this grant is Dr. John C. Knight of the Computer Science Department, University of Virginia, Charlottesville, Virginia 22903.

Research in the year covered by this reporting period has been primarily directed toward the following areas:

- Continued development of mock-ups of computer screens to be used by human operators for a digital reactor control system.
- Development of a reactor simulation to permit testing of the various elements of the control system.
- Formal specification of user interfaces.
- Fault-tree analysis including software.
- Evaluation of formal specification notations.
- Evaluation of formal verification techniques.
- Continued development of a software documentation system.

This report summarizes activities under the grant. The technical results relating to this grant and the remainder of the principal investigator's research program are contained in various reports and papers.

The remainder of this report is organized as follows. In the next section, an overview of the project is given. This is followed by a summary of accomplishments during the reporting period and details of students funded. Seminars presented describing work under this grant are listed in the following section, and the final section lists publications resulting from this grant.

OVERVIEW

The goal of this research is to continue the development of a comprehensive approach to software safety and to evaluate the approach with two case studies. The case studies are a major part of the project, and they involve the analysis of specific safety-critical systems—one from the medical equipment domain and one from the nuclear power domain. The particular applications being used were selected because of the availability of suitable candidate systems. We consider the results to be generally applicable and in no way particularly limited by the domains.

With more and more important functions in existing and proposed safety-critical systems being implemented by computers, concern over the role of software in such systems has increased. An especially important area is that class of systems for which safety rather than reliability or availability is the overriding issue. Some research that addresses the safety of software specifically has been reported but many open questions remain. In particular, no complete process is available for engineers to follow when building applications software for systems in which safety considerations dominate. We are developing such a process through a combination of theoretical and empirical research.

The research is concentrating on issues raised by the specification and verification phases of the software lifecycle. The theoretical research is based on our framework of definitions for software safety in which the problem is broken down into *specification safety* and *implementation safety*.

In the area of specification, the main topics being investigated are:

- the development of a comprehensive technique for specification capture,
- the formal specification of complex user interfaces,
- the reuse of specifications through the development of certified libraries of reusable specification components, and
- the development of rigorous techniques for the preparation of software safety specifications.

A second area of theoretical investigation is the development of verification methods tailored to the characteristics of safety requirements. Verification of the correct implementation of the safety specification is central to the goal of establishing safe software. In the area of specification, the main topics being investigated are:

- the application of *specification limitation* to permit certain classes of safety problems to be eliminated by exhaustive testing in reasonable amounts of time, and
- the development of a complete test set for certain properties by automatic derivation from the safety specifications for specifications written in a suitably formal notation such as 'Z'.

The empirical component of this research is focusing on two case studies in order to provide detailed characterizations of the issues as they appear in practice, and to provide a testbed for the evaluation of various existing and new theoretical results, tools and techniques. The systems being used in the case studies are the *Magnetic Stereotaxis System* (MSS), a safety-critical medical system presently under development and the *University of Virginia's research nuclear reactor* (UVAR). The overall, long term approach being taken in the empirical research using these systems is to develop fully functional software of sufficient quality to be suitable for safety-critical use. This approach is necessary to ensure that the research undertaken is not weakened by unrealistic assumptions or restrictions. The empirical research is implementing the various techniques resulting from the theoretical research and using these implementations to assess the theoretical results.

The focus during the reporting period has been the UVAR case study. Despite the body of existing work, the exploitation of computers in nuclear control systems is not extensive. More specifically, the use of formal software specifications has been undertaken only rarely even though it is well known that specification errors are the most common types of error in safety-critical systems and that formal specifications are capable of far greater precision than natural language. A good example of careful specification is the work of Parnas on the Darlington project. An example of the use of informal specification in a modern system is Sizewell B in the United Kingdom in which the entire system is specified in natural language.

The goal is to determine the utility of formal specifications in digital nuclear system. With the help of members of the staff of the University's reactor facility and the Department of Mechanical, Nuclear and Aerospace Engineering, experiments are being undertaken in which formal specifications are being prepared for parts of an advanced reactor control system.

The control requirements of the reactor are being studied to determine the requirements for emergency shutdown, monitoring and operation, and safe operation including the response to a variety of equipment failures. System fault trees are being developed for certain parts of the system to permit detailed documentation of the software's failure response requirements to be acquired.

Formal specifications for the different control requirements are being prepared. To gain insight into the differences between different approaches and notations, several specifications using different notations are being built for part of the control system. Notations being used include Z, PVS, Statecharts, and SCR. As part of the assessment of the techniques for nuclear applications, experiments are being undertaken to gauge the utility of the notations to nuclear engineers and others.

Research results to date are documented in various papers and reports, and they are not repeated here. Copies of these papers and reports have been supplied to the sponsor under separate cover.

ACCOMPLISHMENTS DURING REPORTING PERIOD

The accomplishments in the various activity areas are summarized in this section. More details of the work in the different activity areas are contained in the publications listed in a later section of this report.

Although much of the work undertaken during the reporting period has focused on the nuclear-reactor case study, this is not a limitation in any sense because our goal is research in software engineering for control systems in general. The proposed control system for the reactor is quite typical in its software requirements.

Control System Operator Interface

The operator interface for the advanced control system has been refined considerably and extended to include several new instruments. The resulting displays have been shown to lead reactor operators for comment and further modified to implement their comments. An example of the changes that have been made is the replacement of analog displays that were composed of a colored strip that represented the analog value with graphics that resemble traditional end-on analog gauges.

This process is incomplete in that further demonstrations are planned and further revisions might be undertaken. In addition, the entire prototype control system including both the operator interface implementation and the reactor simulation have been made available to Professor A. Dearden of the University of York, UK. Professor Dearden will be conducting a research program in the ergonomics of safe user interfaces using the reactor as a case study.

Many details of the operator interface design are documented in the B.S. thesis of Mr. C. Odell (see list of publications).

Reactor Simulation

A self-contained program has been written that accurately models the operation of the UVAR. This simulation program operates in real time and accepts the same set of control commands as the real system. The simulation uses reactivity tables based on actual measurements of the UVAR with its current core configuration thereby ensuring that the fidelity of the simulation is very high.

The simulation executes on a separate computer and communicates with the remainder of the control system over a socket-based network connection. All interfaces are hidden so that a transition to any form of hardware interface will be easy to accomplish.

The simulation has its own control panel that permits a wide variety of failures to be injected under operator control. In addition, the simulation can be controlled from a script contained in a file so that precise sequences of failure events can be repeated.

Many details of the reactor simulator design are documented in the B.S. thesis of Mr. E. Niebler (see list of publications).

User Interface Specification

A key component of any safety-critical system is the user interface. To be sure that the interface works as required, it is essential that it be specified with great care. Despite this, formal specification of user interfaces has not been explored as aggressively as other areas of safety-critical systems. Along with Dr. S. Brilliant of Virginia Commonwealth University (Richmond, VA), the principal investigator has continued research on the formal specification of user interfaces. Large sections of the required user interfaces for the UVAR control system have been formally specified and the approach is being evaluated. An implementation derived from the formal specification is also being prepared.

The work to date in this area has been documented in two conference papers (see list of publications). A third has been submitted.

Comprehensive Fault-Tree Analysis

The system fault tree is the primary model that is used to determine the risks associated with the various system hazards. Fault-tree analysis is used to refine system designs to permit reductions in risk levels where these levels are above acceptable thresholds. For systems that involve software, the introduction of software events into fault trees has proved problematic. The issue is the difficulty of quantifying failure probabilities for software. Since the fault-tree model is the primary technique for risk analysis, it is essential that it be possible to analyze fault trees for systems that depend on software. In addition, it should be noted that the fault tree can and should have a heavy influence on the specification for the software for a system. Thus a system fault tree is a primary input to software specification. With this in mind, we have started to develop techniques for dealing with software in fault trees using a variety of approaches including formal verification, robust design, and exhaustive testing.

Formal Specification

A major goal of the project that we are undertaking is to determine the utility of formal specification techniques in industrial applications. To that end, we have prepared specifications of part of a hypothetical control system for the University's research reactor in four formal notations. They are Z, PVS, Statecharts, and SCR. We have also developed a framework for evaluation of these notations and will be subjecting the notations to evaluation using the reactor case study as an example in the near future.

Formal Verification

A secondary goal of the project is to evaluate the utility of other aspects of formal methods. In parallel with our evaluation of the formal notations, we are evaluating the analysis capabilities that are available for formal notations. These capabilities include type checking, specification analysis, and formal verification. We have developed a framework for evaluation of these analysis capabilities and, again using the research reactor as an example, we will be subjecting the techniques to evaluation in the near future.

Software Documentation

We have continued our development of a software documentation system based on information retrieval technology. The operational system was demonstrated to representatives of the Nuclear Regulatory Commission and the National Institute of Standards Technology. The work has been reported in a conference paper and a journal paper.

SUPPORTED STUDENTS

During the reporting period, the following students were supported in whole or in part under this grant:

Name	-	Luis G. Nakano
Dissertation Title	-	Techniques for the Design and Safety- Analysis of Computer-Based Systems.
Degree	-	Ph.D.
Status	-	In progress

Name	-	Colleen Dejong
Thesis Title	-	TBD
Degree	-	M.S.
Status	-	In progress

Name	-	Matthew Gible
MS Thesis Title	-	TBD
Degree	-	M.S.
Status	-	In progress

Name	-	Eric Niebler
BS Thesis Title	-	The Simulation of a Nuclear Reactor
Degree	-	B.S.
Status	-	Graduated May, 1996

Name	-	Allison Powell
Dissertation Title	-	TBD
Degree	-	Ph.D.
Status	-	In progress

Name	-	Charles Odell
BS Thesis Title	-	A User Interface for a Nuclear Control Software System
Degree	-	B.S.
Status	-	Graduated May 1996

Name	-	Meng Yin
BS Thesis Title	-	TBD
Degree	-	B.S.
Status	-	In progress

Name	-	Zachariah Kohn
BS Thesis Title	-	TBD
Degree	-	B.S.
Status	-	In progress

PRESENTATIONS GIVEN

Seminars describing the research being performed under this grant were presented at the following institution during the reporting period:

- NASA's validation and verification research center, Fairmont WV.

PUBLICATIONS

During the reporting period, the following papers and documents were prepared from the principal investigator's research program[†]:

1. Knight J.C., "Limitations of Mathematics in Software Engineering", *MDS '95, Conference on the Mathematics of Dependable Systems*, Institute of Mathematics and its Applications, September 1995, York, England.
2. Knight, J.C., K.G. Wika, and S.D. Wrege, "Exhaustive Testing as a Verification Technique", TR-95-41 (September 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903.
3. Knight, J.C., and A.G. Cass, "Achieving Software Quality Through Reuse", TR-95-40 (September 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903.
4. Elder, M.C. and J.C. Knight, "Specification of User Interfaces for Safety-Critical Systems", *MRCAS '95, Second International Symposium on Medical Robotics and Computer Assisted Surgery*, November 1995, Baltimore, MD.
5. A. L. Powell, A. J.C. French, J. C. Knight, "A Systematic Approach to Creating and Maintaining Software Documentation", *Proceedings of the 1996 ACM Symposium on Applied Computing*, February 1996, Philadelphia, PA.
6. Sullivan K.J., and J.C. Knight, "Assessment of an Architectural Approach to Large-Scale Systematic Reuse", *ICSE 18: Eighteenth International Conference on Software Engineering*, March 1996, Berlin, Germany.
7. Brilliant, S.S., J.C. Knight, and M.E. Elder, "Formal Specification of a User Interface", *American Nuclear Society Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies*, May 1996, University Park, PA.
8. Odell, C., "A User Interface for a Nuclear Control Software System", B.S. Thesis, School of Engineering and Applied Science, University of Virginia, Charlottesville, VA 22903.
9. Niebler, E., "The Simulation of a Nuclear Reactor", B.S. Thesis, School of Engineering and Applied Science, University of Virginia, Charlottesville, VA 22903.
10. French, J.C., J. C. Knight, A. L. Powell, "Applying Hypertext Structures to Software Documentation" *Journal of Information Processing and Management*, special issue on Methods and Tools for the Automatic Construction of Hypermedia, to appear.

[†]. This list includes all publications attributed to all sponsors.

DISTRIBUTION LIST

- 1 - 3 Dr. Dave E. Eckhardt, MS 478
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-0001
(804) 864-1698
- 4 Mr. Joseph S. Murray, Grants Officer, MS 126
Acquisition Division
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-0001
(804) 864-7709
- 5 - 6* National Aeronautics and Space Administration
Scientific and Technical Information Facility
P. O. Box 8757
Baltimore/Washington International Airport
Baltimore, MD 21240
- 7 - 8 J. C. Knight
- 9 A. P. Batson
- 10 - 11 M. Rodeffer
- ** SEAS Postaward Research Administration
- 12 SEAS Preaward Research Administration

*1 unbound copy

**Cover letter

JO#7331:ph